Title (en)
COMPUTER-SECURITY EVENT SECURITY-VIOLATION DETECTION

Title (de)
SICHERHEITSVERLETZUNGSERKENNUNG EINES COMPUTERSICHERHEITSEREIGNISSES

Title (fr)
DÉTECTION DE VIOLATIONS DE LA SÉCURITÉ D'ÉVÉNEMENTS DE SÉCURITÉ INFORMATIQUE

Publication
EP 3654216 B1 20210728 (EN)

Application
EP 19207848 A 20191107

Priority
US 201816192251 A 20181115

Abstract (en)
[origin: EP3654216A1] Example techniques herein determine that an event associated with a monitored computing device is associated with a security violation. Terms are extracted from at least two command lines associated with the event. Term representations of the at least two terms are determined based at least in part on a trained representation mapping. Two or more first filter outputs are determined based at least in part on the term representations of terms in a respective first subset of the terms. An indication of whether the event is associated with a security violation is determined at least partly by operating a trained classification computational model (CM) based at least in part on the two or more first filter outputs. Various examples train a word2vec or other x2vec model to provide the representation mapping. Various examples train a CM having convolutional and classification sections to provide the indication.

IPC 8 full level
G06F 21/55 (2013.01)

CPC (source: EP US)
G06F 9/542 (2013.01 - US); **G06F 11/3006** (2013.01 - US); **G06F 11/3072** (2013.01 - US); **G06F 18/24** (2023.01 - US);
G06F 21/554 (2013.01 - EP US); **G06F 21/566** (2013.01 - US); **G06F 40/157** (2020.01 - US); **G06F 40/284** (2020.01 - US);
G06N 3/02 (2013.01 - US); **H04L 63/1416** (2013.01 - US); **H04L 63/1441** (2013.01 - US); G06F 2201/86 (2013.01 - US);
G06F 2201/875 (2013.01 - US)

Cited by
CN114218034A; CN111967343A; EP3674948B1

Designated contracting state (EPC)
AL AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HR HU IE IS IT LI LT LU LV MC MK MT NL NO PL PT RO RS SE SI SK SM TR

DOCDB simple family (publication)
EP 3654216 A1 20200520; **EP 3654216 B1 20210728**; US 11062024 B2 20210713; US 2020159916 A1 20200521

DOCDB simple family (application)
EP 19207848 A 20191107; US 201816192251 A 20181115